

Title (en)

Authentication method and system encrypting a ticket with an symmetric key, said symmetric key being encrypted with an asymmetric key

Title (de)

Authentifizierungsverfahren und Vorrichtung zur verschlüsselt eines Tickets mit einem symmetrisch Schlüssel, wobei der symmetrisch Schlüssel mit einem asymmetrisch Schlüssel verschlüsselt ist

Title (fr)

Méthode et système d'authentification avec chiffrement d'un ticket par une clé symétrique, la dite clé étant chiffrée avec une clé asymétrique

Publication

EP 1363424 A3 20040519 (EN)

Application

EP 03007961 A 20030409

Priority

US 14668602 A 20020515

Abstract (en)

[origin: EP1363424A2] A security authentication method and system. After authenticating a user, an authentication server generates a ticket including information associated to the user. The authentication server encrypts the ticket using a symmetric key shared with an affiliated server. The affiliate server has a private key associated with the public key that the authentication server uses to encrypt the symmetric key. The authentication server uses the private key for creating a signature of the ticket. The affiliate server decrypts the symmetric key with its private key and then decrypts the ticket using the decrypted symmetric key. The affiliate server validates the signature by using the authentication server's public key. <IMAGE>

IPC 1-7

H04L 9/08; **H04L 9/32**; **G06F 1/00**; **H04L 29/06**

IPC 8 full level

G06F 21/20 (2006.01); **G06F 21/00** (2006.01); **H04L 9/08** (2006.01); **H04L 9/32** (2006.01); **H04L 29/06** (2006.01)

CPC (source: EP KR US)

G06F 21/33 (2013.01 - EP US); **G06F 21/41** (2013.01 - EP US); **H04L 9/0844** (2013.01 - EP US); **H04L 9/30** (2013.01 - KR); **H04L 9/3213** (2013.01 - EP US); **H04L 9/3247** (2013.01 - EP US); **H04L 63/0807** (2013.01 - EP US); **H04L 63/0815** (2013.01 - EP US); **H04L 63/045** (2013.01 - EP US); **H04L 2209/60** (2013.01 - EP US)

Citation (search report)

- [X] WO 0233884 A2 20020425 - SUN MICROSYSTEMS INC [US]
- [A] US 2001034841 A1 20011025 - SHAMBROOM W DAVID [US]
- [X] US 5535279 A 19960709 - SEESTROM FRANK E [US]
- [A] US 6148404 A 20001114 - YATSUKAWA NAONOBU [JP]
- [X] EP 0969366 A1 20000105 - SUN MICROSYSTEMS INC [US]
- [A] US 6088451 A 20000711 - HE JINGSHA [US], et al
- [A] WO 0177775 A2 20011018 - VIDUIUS INC [US], et al
- [X] STEINER J G ET AL: "KERBEROS: AN AUTHENTICATION SERVICE FOR OPEN NETWORK SYSTEMS", PROCEEDINGS OF THE WINTER USENIX CONFERENCE, XX, XX, 9 February 1988 (1988-02-09), pages 191 - 202, XP000671489

Cited by

EP1610202A1; CN113630261A; EP1697818A4; KR100986441B1; EP2391087A1; EP2863612A4; EP2150887A4; EP2530618A1; WO2005062989A2; US8474009B2; US7552322B2; US9473938B2

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT SE SI SK TR

DOCDB simple family (publication)

EP 1363424 A2 20031119; **EP 1363424 A3 20040519**; **EP 1363424 B1 20080702**; AT E400108 T1 20080715; DE 60321854 D1 20080814; JP 2004048679 A 20040212; JP 4744785 B2 20110810; KR 100986441 B1 20101008; KR 20030088855 A 20031120; US 2003217288 A1 20031120; US 2009204808 A1 20090813; US 7523490 B2 20090421; US 7971240 B2 20110628

DOCDB simple family (application)

EP 03007961 A 20030409; AT 03007961 T 20030409; DE 60321854 T 20030409; JP 2003109094 A 20030414; KR 20030022923 A 20030411; US 14668602 A 20020515; US 42672609 A 20090420